Práctica-(Tarea)
AUDITORÍA DEL SISTEMA

Alejandro Garcia Burguillos

09/10/2024

Instrucciones:

1. Instalación de Lynis (Linux)

1. Abre una terminal en el sistema Linux.
2. Actualiza los repositorios del sistema:
   ```
   sudo apt update
   ```
3. Instala Lynis:
   https://cisofy.com/lynis
4. Ejecuta Lynis para realizar una auditoría completa del sistema:
   El comando generará un informe con varias recomendaciones de seguridad.
   Guarda el informe en un archivo para su análisis.

2. Instalación de CLARA (Windows)

1. Descarga CLARA desde el siguiente enlace:
   https://www.ccn-cert.cni.es/soluciones-seguridad/clara.html
2. Descomprime el archivo descargado e instala la herramienta en tu sistema Windows.
3. Ejecuta CLARA y realiza una auditoría completa del sistema.
4. Guarda el informe de CLARA en un archivo.

3. Instalación de Nessus (Linux/Windows)

1. Descarga Nessus desde el siguiente enlace: https://es-la.tenable.com

   https://www.tenable.com/tenable-for-education/nessus-essentials

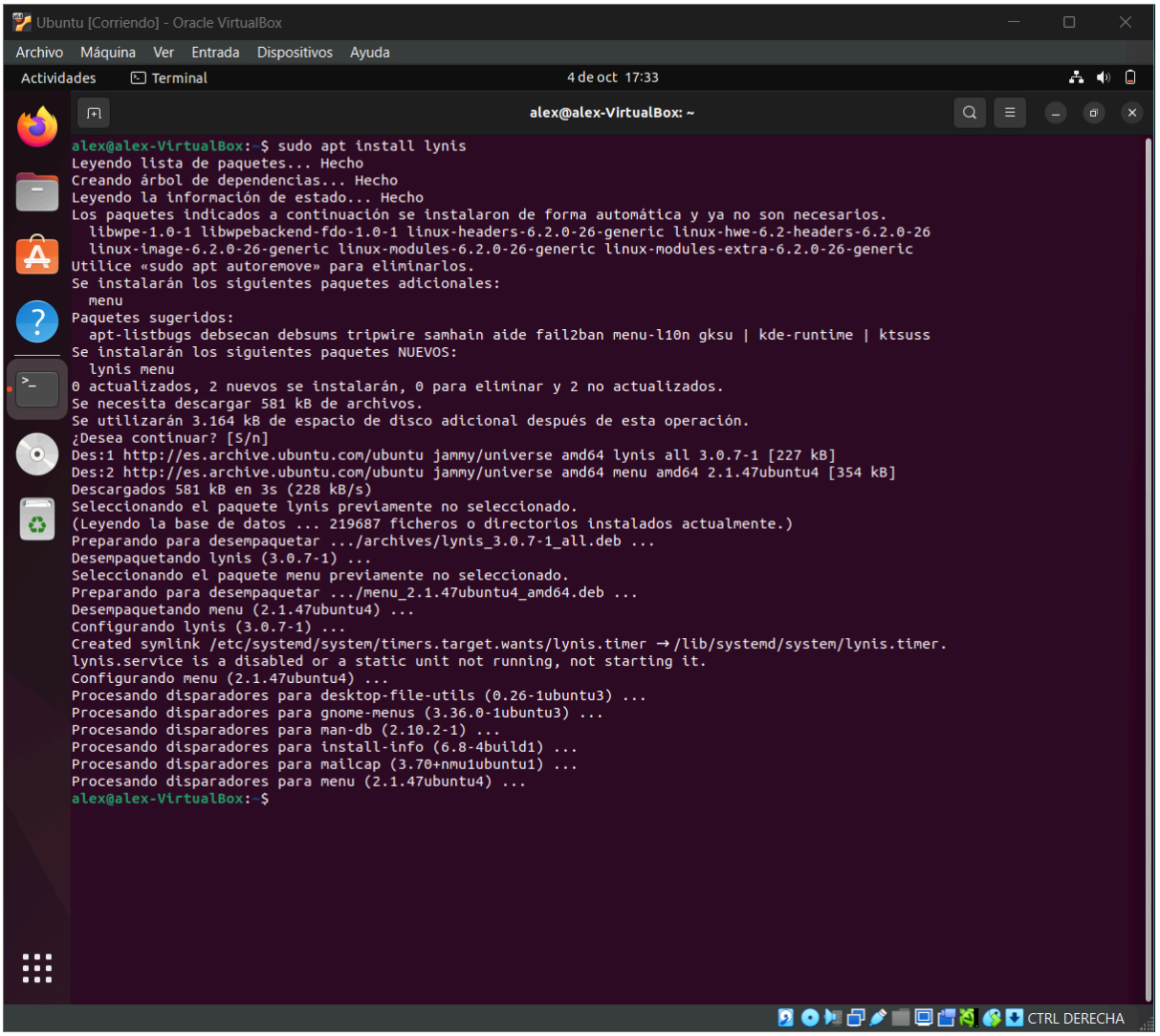
2. Selecciona la versión de prueba gratuita de Nessus.
3. Sigue las instrucciones de instalación para tu sistema operativo (puede ser tanto en Linux como en Windows).
4. Una vez instalado, abre Nessus desde el navegador web, donde te pedirá registrar una cuenta.
5. Configura y realiza un escaneo de vulnerabilidades en los mismos sistemas donde ejecutaste Lynis y CLARA.
6. Guarda los informes de los resultados.

PUNTO 1.

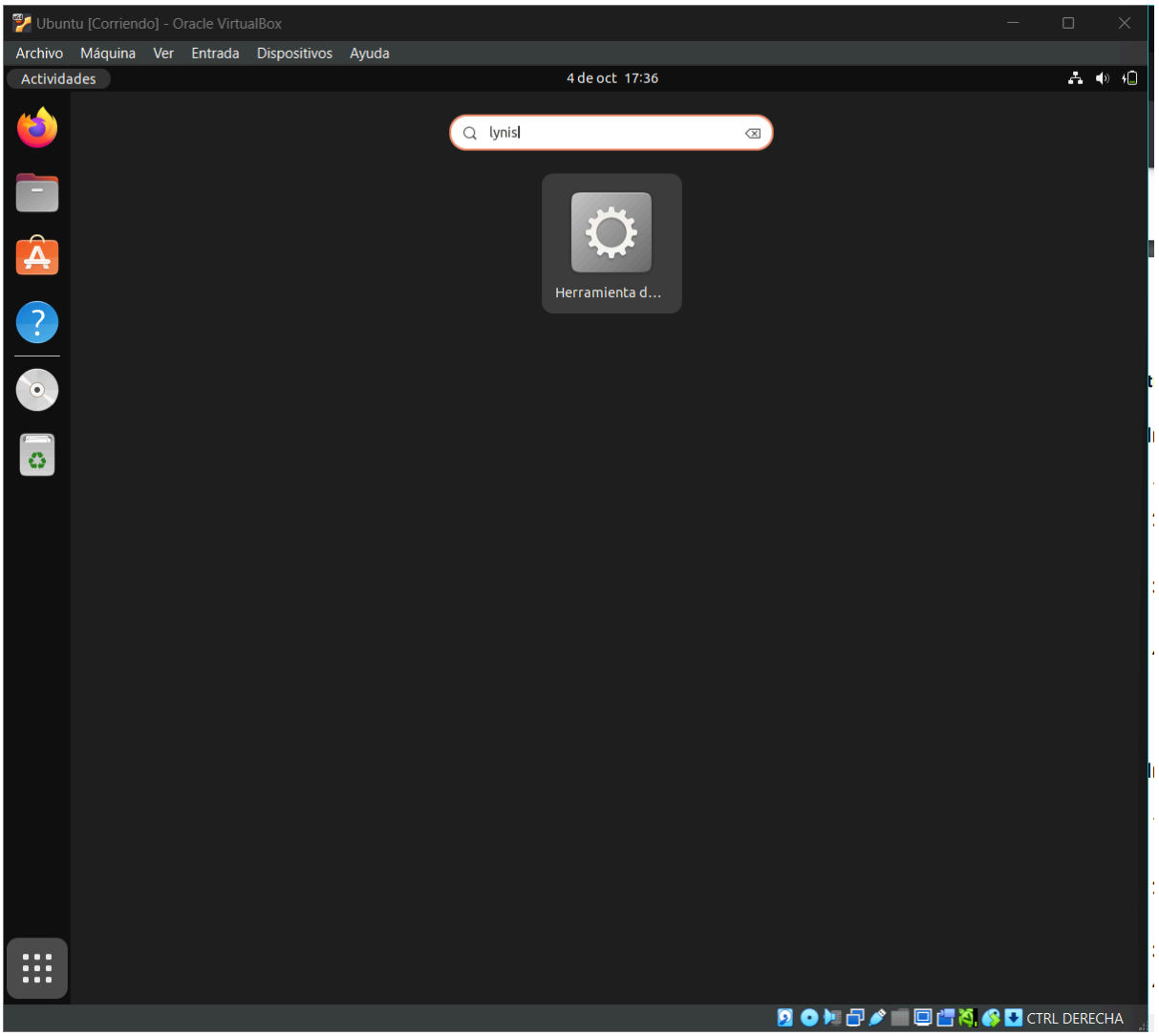
Primero vamos a instalar **Linys**, para ello, iniciaremos ubuntu y lo actualizaremos, para actualizar, ponemos lo siguiente en consola: “sudo apt update”.

Después de actualizar ponemos: “sudo apt upgrade”.

Una vez terminado instalamos **Linys** para ello en consola ponemos: “sudo apt install lynis”.



Una vez instalado ya podremos usar **Linys,** solo tendremos que irnos abajo a la izquierda y escribir Linys, ahí encontraremos su acceso, lo abrimos y se nos abrirá una ventana de consola donde realizará la auditoría.



Cuando termina la auditoría se cierra la ventana automáticamente por lo que para ver el registro que deja la auditoría escribimos en consola esta linea: **“sudo /usr/sbin/lynis audit system --no-colors >> ~/Documentos/Auditoria-Lynis.txt”**.

Esto guardará la auditoría en un txt que posteriormente podremos ver tranquilamente.

Auditoría Lynis:

[Lynis 3.0.7]

##

Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are

welcome to redistribute it under the terms of the GNU General Public License.

See the LICENSE file for details about using this software.

2007-2021, CISOfy - https://cisofy.com/lynis/

Enterprise support available (compliance, plugins, interface and tools)

##

[+] Initializing program

[2C- Detecting OS... [41C [DONE]

[2C- Checking profiles...[37C [DONE]

[2C- Detecting language and localization[22C [es]

Program version: 3.0.7

Operating system: Linux

Operating system name: Ubuntu

Operating system version: 22.04

Kernel version: 6.8.0

Hardware platform: x86_64

Hostname: alex-VirtualBox

Profiles: /etc/lynis/default.prf

Log file: /var/log/lynis.log

Report file: /var/log/lynis-report.dat

Report version: 1.0

Plugin directory: /etc/lynis/plugins

Auditor: [Not Specified]

Language: es

Test category: all

Test group: all

[2C- Program update status... [32C [SIN ACTUALIZACIÓN]

[+] Herramientas del sistema

[2C- Scanning available tools...[30C

[2C- Checking system binaries...[30C

[+] Plugins (fase 1)

[0CNota: los plugins contienen pruebas más extensivas y toman más tiempo[0C

[0C [0C

[2C- Plugin: debian[43C

[

[+] Debian Tests

[2C- Checking for system binaries that are required by Debian Tests...[0C

[4C- Checking /bin... [38C [FOUND]

[4C- Checking /sbin... [37C [FOUND]

[4C- Checking /usr/bin... [34C [FOUND]

[4C- Checking /usr/sbin... [33C [FOUND]

[4C- Checking /usr/local/bin... [28C [FOUND]

[4C- Checking /usr/local/sbin... [27C [FOUND]

[2C- Authentication:[42C

[4C- PAM (Pluggable Authentication Modules):[16C

[WARNING]: Test DEB-0001 had a long execution: 14.281109 seconds

[6C- libpam-tmpdir[40C [Not Installed]

[2C- File System Checks:[38C

[4C- DM-Crypt, Cryptsetup & Cryptmount:[21C

[2C- Software:[48C

[4C- apt-listbugs[43C [Not Installed]

[4C- apt-listchanges[40C [Not Installed]

[4C- needrestart[44C [Not Installed]

[4C- fail2ban[47C [Not Installed]

]

[+] Arranque y servicios

[2C- Service Manager[42C [systemd]

[2C- Checking UEFI boot[39C [DESHABILITADO]

[2C- Checking presence GRUB2[34C [ENCONTRADO]

[4C- Checking for password protection[23C [NINGUNO]

[2C- Check running services (systemctl)[23C [HECHO]

[8CResult: found 33 running services[20C

[2C- Check enabled services at boot (systemctl)[15C [HECHO]

[8CResult: found 51 enabled services[20C

[2C- Check startup files (permissions)[24C [OK]

[2C- Running 'systemd-analyze security'[23C

[8C- ModemManager.service:[30C [MEDIO]

[8C- NetworkManager.service:[28C [EXPUESTO]

[8C- accounts-daemon.service:[27C [MEDIO]

[8C- acpid.service:[37C [INSEGURO]

[8C- alsa-state.service:[32C [INSEGURO]

[8C- anacron.service:[35C [INSEGURO]

[8C- apport.service:[36C [INSEGURO]

[8C- avahi-daemon.service:[30C [INSEGURO]

[8C- colord.service:[36C [EXPUESTO]

[8C- cron.service:[38C [INSEGURO]

[8C- cups-browsed.service:[30C [INSEGURO]

[8C- cups.service:[38C [INSEGURO]

[8C- dbus.service:[38C [INSEGURO]

[8C- dmesg.service:[37C [INSEGURO]

[8C- emergency.service:[33C [INSEGURO]

[8C- gdm.service:[39C [INSEGURO]

[8C- getty@tty1.service:[32C [INSEGURO]

[8C- irqbalance.service:[32C [MEDIO]

[8C- kerneloops.service:[32C [INSEGURO]

[8C- lynis.service:[37C [INSEGURO]

[8C- networkd-dispatcher.service:[23C [INSEGURO]

[8C- open-vm-tools.service:[29C [INSEGURO]

[8C- packagekit.service:[32C [INSEGURO]

[8C- plymouth-start.service:[28C [INSEGURO]

[8C- polkit.service:[36C [INSEGURO]

[8C- power-profiles-daemon.service:[21C [EXPUESTO]

[8C- rc-local.service:[34C [INSEGURO]

[8C- rescue.service:[36C [INSEGURO]

[8C- rsyslog.service:[35C [INSEGURO]

[8C- rtkit-daemon.service:[30C [MEDIO]

[8C- snapd.service:[37C [INSEGURO]

[8C- switcheroo-control.service:[24C [EXPUESTO]

[8C- systemd-ask-password-console.service:[14C [INSEGURO]

[8C- systemd-ask-password-plymouth.service:[13C [INSEGURO]

[8C- systemd-ask-password-wall.service:[17C [INSEGURO]

[8C- systemd-fsckd.service:[29C [INSEGURO]

[8C- systemd-initctl.service:[27C [INSEGURO]

[8C- systemd-journald.service:[26C [PROTEGIDO]

[8C- systemd-logind.service:[28C [PROTEGIDO]

[8C- systemd-networkd.service:[26C [PROTEGIDO]

[8C- systemd-oomd.service:[30C [PROTEGIDO]

[8C- systemd-resolved.service:[26C [PROTEGIDO]

[8C- systemd-rfkill.service:[28C [INSEGURO]

[8C- systemd-timesyncd.service:[25C [PROTEGIDO]

[8C- systemd-udevd.service:[29C [MEDIO]

[8C- thermald.service:[34C [INSEGURO]

[8C- ubuntu-advantage.service:[26C [INSEGURO]

[8C- udisks2.service:[35C [INSEGURO]

[8C- unattended-upgrades.service:[23C [INSEGURO]

[8C- upower.service:[36C [PROTEGIDO]

[8C- user@1000.service:[33C [INSEGURO]

[8C- uuidd.service:[37C [PROTEGIDO]

[8C- vboxadd-service.service:[27C [INSEGURO]

[8C- vgauth.service:[36C [INSEGURO]

[8C- whoopsie.service:[34C [INSEGURO]

[8C- wpa_supplicant.service:[28C [INSEGURO]

[+] Kernel

[2C- Checking default run level[31C [RUNLEVEL 5]

[2C- Checking CPU support (NX/PAE)[28C

[4CCPU support: PAE and/or NoeXecute supported[14C [ENCONTRADO]

[2C- Checking kernel version and release[22C [HECHO]

[2C- Checking kernel type[37C [HECHO]

[2C- Checking loaded kernel modules[27C [HECHO]

[6CFound 64 active modules[32C

[2C- Checking Linux kernel configuration file[17C [ENCONTRADO]

[2C- Checking default I/O kernel scheduler[20C [NO ENCONTRADO]

[2C- Checking for available kernel update[21C [OK]

[2C- Checking core dumps configuration[24C

[4C- configuration in systemd conf files[20C [POR DEFECTO]

[4C- configuration in etc/profile[27C [POR DEFECTO]

[4C- 'hard' configuration in security/limits.conf[11C [POR DEFECTO]

[4C- 'soft' configuration in security/limits.conf[11C [POR DEFECTO]

[4C- Checking setuid core dumps configuration[15C [PROTEGIDO]

[2C- Check if reboot is needed[32C [NO]

[+] Memoria y procesos

[2C- Checking /proc/meminfo[35C [ENCONTRADO]

[2C- Searching for dead/zombie processes[22C [NO ENCONTRADO]

[2C- Searching for IO waiting processes[23C [NO ENCONTRADO]

[2C- Search prelink tooling[35C [NO ENCONTRADO]

[+] Usuarios, grupos y autenticación

[2C- Administrator accounts[35C [OK]

[2C- Unique UIDs[46C [OK]

[2C- Consistency of group files (grpck)[23C [OK]

[2C- Unique group IDs[41C [OK]

[2C- Unique group names[39C [OK]

[2C- Password file consistency[32C [OK]

[2C- Password hashing methods[33C [OK]

[2C- Checking password hashing rounds[25C [DESHABILITADO]

[2C- Query system users (non daemons)[25C [HECHO]

[2C- NIS+ authentication support[30C [NO HABILITADO]

[2C- NIS authentication support[31C [NO HABILITADO]

[2C- Sudoers file(s)[42C [ENCONTRADO]

[4C- Permissions for directory: /etc/sudoers.d[14C [PELIGRO]

[4C- Permissions for: /etc/sudoers[26C [OK]

[4C- Permissions for: /etc/sudoers.d/README[17C [OK]

[2C- PAM password strength tools[30C [OK]

[2C- PAM configuration files (pam.conf)[23C [ENCONTRADO]

[2C- PAM configuration files (pam.d)[26C [ENCONTRADO]

[2C- PAM modules[46C [ENCONTRADO]

[2C- LDAP module in PAM[39C [NO ENCONTRADO]

[2C- Accounts without expire date[29C [SUGERENCIA]

[2C- Accounts without password[32C [OK]

[2C- Locked accounts[42C [OK]

[2C- Checking user password aging (minimum)[19C [DESHABILITADO]

[2C- User password aging (maximum)[28C [DESHABILITADO]

[2C- Checking expired passwords[31C [OK]

[2C- Checking Linux single user mode authentication[11C [OK]

[2C- Determining default umask[32C

[4C- umask (/etc/profile)[35C [NO ENCONTRADO]

[4C- umask (/etc/login.defs)[32C [SUGERENCIA]

[2C- LDAP authentication support[30C [NO HABILITADO]

[2C- Logging failed login attempts[28C [HABILITADO]

[+] Shells

[2C- Checking shells from /etc/shells[25C

[4CResult: found 8 shells (valid shells: 8).[16C

[4C- Session timeout settings/tools[25C [NINGUNO]

[2C- Checking default umask values[28C

[4C- Checking default umask in /etc/bash.bashrc[13C [NINGUNO]

[4C- Checking default umask in /etc/profile[17C [NINGUNO]

[+] Sistemas de ficheros

[2C- Checking mount points[36C

[4C- Checking /home mount point[29C [SUGERENCIA]

[4C- Checking /tmp mount point[30C [SUGERENCIA]

[4C- Checking /var mount point[30C [SUGERENCIA]

[2C- Query swap partitions (fstab)[28C [OK]

[2C- Testing swap partitions[34C [OK]

[2C- Testing /proc mount (hidepid)[28C [SUGERENCIA]

[2C- Checking for old files in /tmp[27C [OK]

[2C- Checking /tmp sticky bit[33C [OK]

[2C- Checking /var/tmp sticky bit[29C [OK]

[2C- ACL support root file system[29C [HABILITADO]

[2C- Mount options of /[39C [NO POR DEFECTO]

[2C- Mount options of /dev[36C [PARCIALMENTE BASTIONADO]

[2C- Mount options of /dev/shm[32C [PARCIALMENTE BASTIONADO]

[2C- Mount options of /run[36C [BASTIONADO]

[2C- Total without nodev:8 noexec:27 nosuid:22 ro or noexec (W^X): 10 of total 45[0C

[2C- Disable kernel support of some filesystems[15C

[+] Dispositivos USB

[2C- Checking usb-storage driver (modprobe config)[12C [NO DESHABILITADO]

[2C- Checking USB devices authorization[23C [HABILITADO]

[2C- Checking USBGuard[40C [NO ENCONTRADO]

[+] Almacenamiento

[2C- Checking firewire ohci driver (modprobe config)[10C [DESHABILITADO]

[+] NFS

[2C- Check running NFS daemon[33C [NO ENCONTRADO]

[+] Servicios de nombres

[2C- Checking search domains[34C [ENCONTRADO]

[2C- Checking /etc/resolv.conf options[24C [ENCONTRADO]

[2C- Searching DNS domain name[32C [DESCONOCIDO]

[2C- Checking /etc/hosts[38C

[4C- Duplicate entries in hosts file[24C [NINGUNO]

[4C- Presence of configured hostname in /etc/hosts[10C [ENCONTRADO]

[4C- Hostname mapped to localhost[27C [NO ENCONTRADO]

[4C- Localhost mapping to IP address[24C [OK]

[+] Puertos y paquetes

[2C- Searching package managers[31C

[4C- Searching dpkg package manager[25C [ENCONTRADO]

[6C- Querying package manager[29C

[WARNING]: Test PKGS-7345 had a long execution: 11.357917 seconds

[4C- Query unpurged packages[32C [NINGUNO]

[2C- Checking security repository in sources.list file[8C [OK]

[2C- Checking APT package database[28C [OK]

[2C- Checking vulnerable packages[29C [OK]

[2C- Checking upgradeable packages[28C [OMITIDO]

[2C- Checking package audit tool[30C [INSTALADO]

[4CFound: apt-check[41C

[2C- Toolkit for automatic upgrades (unattended-upgrade)[6C [ENCONTRADO]

[+] Conectividad

[2C- Checking IPv6 configuration[30C [HABILITADO]

[6CConfiguration method[35C [AUTO]

[6CIPv6 only[46C [NO]

[2C- Checking configured nameservers[26C

[4C- Testing nameservers[36C

[8CNameserver: 127.0.0.53[31C [OK]

[4C- DNSSEC supported (systemd-resolved)[20C [NO]

[2C- Getting listening ports (TCP/UDP)[24C [HECHO]

[2C- Checking promiscuous interfaces[26C [OK]

[2C- Checking status DHCP client[30C

[2C- Checking for ARP monitoring software[21C [NO ENCONTRADO]

[2C- Uncommon network protocols[31C [0]

[+] Impresoras y spools

[2C- Checking cups daemon[37C [CORRIENDO]

[2C- Checking CUPS configuration file[25C [OK]

[4C- File permissions[39C [PELIGRO]

[2C- Checking CUPS addresses/sockets[26C [ENCONTRADO]

[2C- Checking lp daemon[39C [NO ESTÁ CORRIENDO]

[+] Software: correo electrónico y mensajería

[+] Software: firewalls

[2C- Checking iptables kernel module[26C [ENCONTRADO]

[4C- Checking iptables policies of chains[19C [ENCONTRADO]

[4C- Checking for empty ruleset[29C [PELIGRO]

[4C- Checking for unused rules[30C [OK]

[2C- Checking host based firewall[29C [ACTIVO]

[+] Software: servidor web

[2C- Checking Apache[42C [NO ENCONTRADO]

[2C- Checking nginx[43C [NO ENCONTRADO]

[+] Soporte SSH

[2C- Checking running SSH daemon[30C [NO ENCONTRADO]

[+] Soporte SNMP

[2C- Checking running SNMP daemon[29C [NO ENCONTRADO]

[+] Bases de datos

[4CNo database engines found[32C

[+] Servicios LDAP

[2C- Checking OpenLDAP instance[31C [NO ENCONTRADO]

[+] PHP

[2C- Checking PHP[45C [NO ENCONTRADO]

[+] Soporte Squid

[2C- Checking running Squid daemon[28C [NO ENCONTRADO]

[+] Logging y ficheros

[2C- Checking for a running log daemon[24C [OK]

[4C- Checking Syslog-NG status[30C [NO ENCONTRADO]

[4C- Checking systemd journal status[24C [ENCONTRADO]

[4C- Checking Metalog status[32C [NO ENCONTRADO]

[4C- Checking RSyslog status[32C [ENCONTRADO]

[4C- Checking RFC 3195 daemon status[24C [NO ENCONTRADO]

[4C- Checking minilogd instances[28C [NO ENCONTRADO]

[2C- Checking logrotate presence[30C [OK]

[2C- Checking remote logging[34C [NO HABILITADO]

[2C- Checking log directories (static list)[19C [HECHO]

[2C- Checking open log files[34C [HECHO]

[2C- Checking deleted files in use[28C [ARCHIVOS ENCONTRADOS]

[+] Servicios inseguros

[2C- Installed inetd package[34C [NO ENCONTRADO]

[2C- Installed xinetd package[33C [OK]

[4C- xinetd status[42C

[2C- Installed rsh client package[29C [OK]

[2C- Installed rsh server package[29C [OK]

[2C- Installed telnet client package[26C [OK]

[2C- Installed telnet server package[26C [NO ENCONTRADO]

[2C- Checking NIS client installation[25C [OK]

[2C- Checking NIS server installation[25C [OK]

[2C- Checking TFTP client installation[24C [OK]

[2C- Checking TFTP server installation[24C [OK]

[+] Banners e identificación

[2C- /etc/issue[47C [ENCONTRADO]

[4C- /etc/issue contents[36C [DÉBIL]

[2C- /etc/issue.net[43C [ENCONTRADO]

[4C- /etc/issue.net contents[32C [DÉBIL]

[+] Tareas programadas

[2C- Checking crontab and cronjob files[23C [HECHO]

[+] Contabilidad

[2C- Checking accounting information[26C [NO ENCONTRADO]

[2C- Checking sysstat accounting data[25C [NO ENCONTRADO]

[2C- Checking auditd[42C [NO ENCONTRADO]

[+] Tiempo y sincronización

[2C- NTP daemon found: systemd (timesyncd)[20C [ENCONTRADO]

[2C- Checking for a running NTP daemon or client[14C [OK]

[2C- Last time synchronization[32C [25s]

[+] Criptografía

[2C- Checking for expired SSL certificates [0/151][12C [NINGUNO]

[WARNING]: Test CRYP-7902 had a long execution: 18.492491 seconds

[2C- Kernel entropy is sufficient[29C [SÍ]

[2C- HW RNG & rngd[44C [NO]

[2C- SW prng[50C [NO]

[2C- MOR variable not found[35C [DÉBIL]

[+] Virtualización

[+] Contenedores

[+] Frameworks de seguridad

[2C- Checking presence AppArmor[31C [ENCONTRADO]

[4C- Checking AppArmor status[31C [HABILITADO]

[8CFound 120 unconfined processes[23C

[2C- Checking presence SELinux[32C [NO ENCONTRADO]

[2C- Checking presence TOMOYO Linux[27C [NO ENCONTRADO]

[2C- Checking presence grsecurity[29C [NO ENCONTRADO]

[2C- Checking for implemented MAC framework[19C [OK]

[+] Software: integridad de ficheros

[2C- Checking file integrity tools[28C

[2C- Checking presence integrity tool[25C [NO ENCONTRADO]

[+] Software: Herramientas del sistema

[2C- Checking automation tooling[30C

[2C- Automation tooling[39C [NO ENCONTRADO]

[2C- Checking for IDS/IPS tooling[29C [NINGUNO]

[+] Software: Malware

[2C- Malware software components[30C [NO ENCONTRADO]

[+] Permisos de ficheros

[2C- Starting file permissions check[26C

[4CFile: /boot/grub/grub.cfg[32C [SUGERENCIA]

[4CFile: /etc/crontab[39C [SUGERENCIA]

[4CFile: /etc/group[41C [OK]

[4CFile: /etc/group-[40C [OK]

[4CFile: /etc/hosts.allow[35C [OK]

[4CFile: /etc/hosts.deny[36C [OK]

[4CFile: /etc/issue[41C [OK]

[4CFile: /etc/issue.net[37C [OK]

[4CFile: /etc/passwd[40C [OK]

[4CFile: /etc/passwd-[39C [OK]

[4CDirectory: /etc/cron.d[35C [SUGERENCIA]

[4CDirectory: /etc/cron.daily[31C [SUGERENCIA]

[4CDirectory: /etc/cron.hourly[30C [SUGERENCIA]

[4CDirectory: /etc/cron.weekly[30C [SUGERENCIA]

[4CDirectory: /etc/cron.monthly[29C [SUGERENCIA]

[+] Directorios de inicio

[2C- Permissions of home directories[26C [OK]

[2C- Ownership of home directories[28C [OK]

[2C- Checking shell history files[29C [OK]

[+] Bastionado del kernel

[2C- Comparing sysctl key pairs with scan profile[13C

[4C- dev.tty.ldisc_autoload (exp: 0)[24C [DIFERENTE]

[4C- fs.protected_fifos (exp: 2)[28C [DIFERENTE]

[4C- fs.protected_hardlinks (exp: 1)[24C [OK]

[4C- fs.protected_regular (exp: 2)[26C [OK]

[4C- fs.protected_symlinks (exp: 1)[25C [OK]

[4C- fs.suid_dumpable (exp: 0)[30C [DIFERENTE]

[4C- kernel.core_uses_pid (exp: 1)[26C [OK]

[4C- kernel.ctrl-alt-del (exp: 0)[27C [OK]

[4C- kernel.dmesg_restrict (exp: 1)[25C [OK]

[4C- kernel.kptr_restrict (exp: 2)[26C [DIFERENTE]

[4C- kernel.modules_disabled (exp: 1)[23C [DIFERENTE]

[4C- kernel.perf_event_paranoid (exp: 3)[20C [DIFERENTE]

[4C- kernel.randomize_va_space (exp: 2)[21C [OK]

[4C- kernel.sysrq (exp: 0)[34C [DIFERENTE]

[4C- kernel.unprivileged_bpf_disabled (exp: 1)[14C [DIFERENTE]

[4C- kernel.yama.ptrace_scope (exp: 1 2 3)[18C [OK]

[4C- net.core.bpf_jit_harden (exp: 2)[23C [DIFERENTE]

[4C- net.ipv4.conf.all.accept_redirects (exp: 0)[12C [DIFERENTE]

[4C- net.ipv4.conf.all.accept_source_route (exp: 0)[9C [OK]

[4C- net.ipv4.conf.all.bootp_relay (exp: 0)[17C [OK]

[4C- net.ipv4.conf.all.forwarding (exp: 0)[18C [OK]

[4C- net.ipv4.conf.all.log_martians (exp: 1)[16C [DIFERENTE]

[4C- net.ipv4.conf.all.mc_forwarding (exp: 0)[15C [OK]

[4C- net.ipv4.conf.all.proxy_arp (exp: 0)[19C [OK]

[4C- net.ipv4.conf.all.rp_filter (exp: 1)[19C [DIFERENTE]

[4C- net.ipv4.conf.all.send_redirects (exp: 0)[14C [DIFERENTE]

[4C- net.ipv4.conf.default.accept_redirects (exp: 0)[8C [DIFERENTE]

[4C- net.ipv4.conf.default.accept_source_route (exp: 0)[5C [OK]

[4C- net.ipv4.conf.default.log_martians (exp: 1)[12C [DIFERENTE]

[4C- net.ipv4.icmp_echo_ignore_broadcasts (exp: 1)[10C [OK]

[4C- net.ipv4.icmp_ignore_bogus_error_responses (exp: 1)[4C [OK]

[4C- net.ipv4.tcp_syncookies (exp: 1)[23C [OK]

[4C- net.ipv4.tcp_timestamps (exp: 0 1)[21C [OK]

[4C- net.ipv6.conf.all.accept_redirects (exp: 0)[12C [DIFERENTE]

[4C- net.ipv6.conf.all.accept_source_route (exp: 0)[9C [OK]

[4C- net.ipv6.conf.default.accept_redirects (exp: 0)[8C [DIFERENTE]

[4C- net.ipv6.conf.default.accept_source_route (exp: 0)[5C [OK]

[+] Bastionado

[4C- Installed compiler(s)[34C [NO ENCONTRADO]

[4C- Installed malware scanner[30C [NO ENCONTRADO]

[4C- Non-native binary formats[30C [ENCONTRADO]

[+] Pruebas personalizadas

[2C- Running custom tests... [33C [NINGUNO]

[+] Plugins (fase 2)

==

-[Lynis 3.0.7 Results]-

Warnings (1):

! iptables module(s) loaded, but no rules active [FIRE-4512]

https://cisofy.com/lynis/controls/FIRE-4512/

Suggestions (39):

----

* This release is more than 4 months old. Check the website or GitHub to see if there is an update available. [LYNIS]

https://cisofy.com/lynis/controls/LYNIS/

* Install libpam-tmpdir to set $TMP and $TMPDIR for PAM sessions [DEB-0280]

https://cisofy.com/lynis/controls/DEB-0280/

* Install apt-listbugs to display a list of critical bugs prior to each APT installation. [DEB-0810]

https://cisofy.com/lynis/controls/DEB-0810/

* Install apt-listchanges to display any significant changes prior to any upgrade via APT. [DEB-0811]

https://cisofy.com/lynis/controls/DEB-0811/

* Install needrestart, alternatively to debian-goodies, so that you can run needrestart after upgrades to determine which daemons are using old versions of libraries and need restarting. [DEB-0831]

https://cisofy.com/lynis/controls/DEB-0831/

* Install fail2ban to automatically ban hosts that commit multiple authentication errors. [DEB-0880]

https://cisofy.com/lynis/controls/DEB-0880/

* Set a password on GRUB boot loader to prevent altering boot configuration (e.g. boot in single user mode without password) [BOOT-5122]

https://cisofy.com/lynis/controls/BOOT-5122/

* Consider hardening system services [BOOT-5264]

- Details : Run '/usr/bin/systemd-analyze security SERVICE' for each service

https://cisofy.com/lynis/controls/BOOT-5264/

* If not required, consider explicit disabling of core dump in /etc/security/limits.conf file [KRNL-5820]

https://cisofy.com/lynis/controls/KRNL-5820/

* Configure password hashing rounds in /etc/login.defs [AUTH-9230]

https://cisofy.com/lynis/controls/AUTH-9230/

* When possible set expire dates for all password protected accounts [AUTH-9282]

https://cisofy.com/lynis/controls/AUTH-9282/

* Configure minimum password age in /etc/login.defs [AUTH-9286]

https://cisofy.com/lynis/controls/AUTH-9286/

* Configure maximum password age in /etc/login.defs [AUTH-9286]

https://cisofy.com/lynis/controls/AUTH-9286/

* Default umask in /etc/login.defs could be more strict like 027 [AUTH-9328]

https://cisofy.com/lynis/controls/AUTH-9328/

* To decrease the impact of a full /home file system, place /home on a separate partition [FILE-6310]

https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /tmp file system, place /tmp on a separate partition [FILE-6310]

https://cisofy.com/lynis/controls/FILE-6310/

* To decrease the impact of a full /var file system, place /var on a separate partition [FILE-6310]

  https://cisofy.com/lynis/controls/FILE-6310/

* Disable drivers like USB storage when not used, to prevent unauthorized storage or data theft [USB-1000]

  https://cisofy.com/lynis/controls/USB-1000/

* Check DNS configuration for the dns domain name [NAME-4028]

  https://cisofy.com/lynis/controls/NAME-4028/

* Install debsums utility for the verification of packages with known good database. [PKGS-7370]

  https://cisofy.com/lynis/controls/PKGS-7370/

* Install package apt-show-versions for patch management purposes [PKGS-7394]

  https://cisofy.com/lynis/controls/PKGS-7394/

* Determine if protocol 'dccp' is really needed on this system [NETW-3200]

  https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'sctp' is really needed on this system [NETW-3200]

  https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'rds' is really needed on this system [NETW-3200]

  https://cisofy.com/lynis/controls/NETW-3200/

* Determine if protocol 'tipc' is really needed on this system [NETW-3200]

  https://cisofy.com/lynis/controls/NETW-3200/

* Access to CUPS configuration could be more strict. [PRNT-2307]

  https://cisofy.com/lynis/controls/PRNT-2307/

* Check CUPS configuration if it really needs to listen on the network [PRNT-2308]

  https://cisofy.com/lynis/controls/PRNT-2308/

* Enable logging to an external logging host for archiving purposes and additional protection [LOGG-2154]

  https://cisofy.com/lynis/controls/LOGG-2154/

* Check what deleted files are still in use and why. [LOGG-2190]

  https://cisofy.com/lynis/controls/LOGG-2190/

* Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]

  https://cisofy.com/lynis/controls/BANN-7126/

* Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]

  https://cisofy.com/lynis/controls/BANN-7130/

* Enable process accounting [ACCT-9622]

  https://cisofy.com/lynis/controls/ACCT-9622/

* Enable sysstat to collect accounting (no results) [ACCT-9626]

  https://cisofy.com/lynis/controls/ACCT-9626/

* Enable auditd to collect audit information [ACCT-9628]

  https://cisofy.com/lynis/controls/ACCT-9628/

* Install a file integrity tool to monitor changes to critical and sensitive files [FINT-4350]

  https://cisofy.com/lynis/controls/FINT-4350/

* Determine if automation tools are present for system management [TOOL-5002]

  https://cisofy.com/lynis/controls/TOOL-5002/

* Consider restricting file permissions [FILE-7524]
  - Details : See screen output or log file
  - Solution : Use chmod to change file permissions

  https://cisofy.com/lynis/controls/FILE-7524/

* One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
  - Solution : Change sysctl value or disable test (skip-test=KRNL-6000:<sysctl-key>)

https://cisofy.com/lynis/controls/KRNL-6000/

* Harden the system by installing at least one malware scanner, to perform periodic file system scans [HRDN-7230]

- Solution : Install a tool like rkhunter, chkrootkit, OSSEC

https://cisofy.com/lynis/controls/HRDN-7230/

Follow-up:

- Show details of a test (lynis show details TEST-ID)

- Check the logfile for all details (less /var/log/lynis.log)

- Read security controls texts (https://cisofy.com)

- Use --upload to upload data to central system (Lynis Enterprise users)

==========

Lynis security scan details:

Hardening index : 65 [##############]

Tests performed : 248

Plugins enabled : 1

Components:

- Firewall [V]

- Malware scanner [X]

Scan mode:

Normal [V] Forensics [ ] Integration [ ] Pentest [ ]

Lynis modules:

- Compliance status [?]

- Security audit [V]

- Vulnerability scan [V]

Files:

- Test and debug information : /var/log/lynis.log

- Report data : /var/log/lynis-report.dat

==========

Lynis 3.0.7

Auditing, system hardening, and compliance for UNIX-based systems

(Linux, macOS, BSD, and others)

2007-2021, CISOfy - https://cisofy.com/lynis/

Enterprise support available (compliance, plugins, interface and tools)

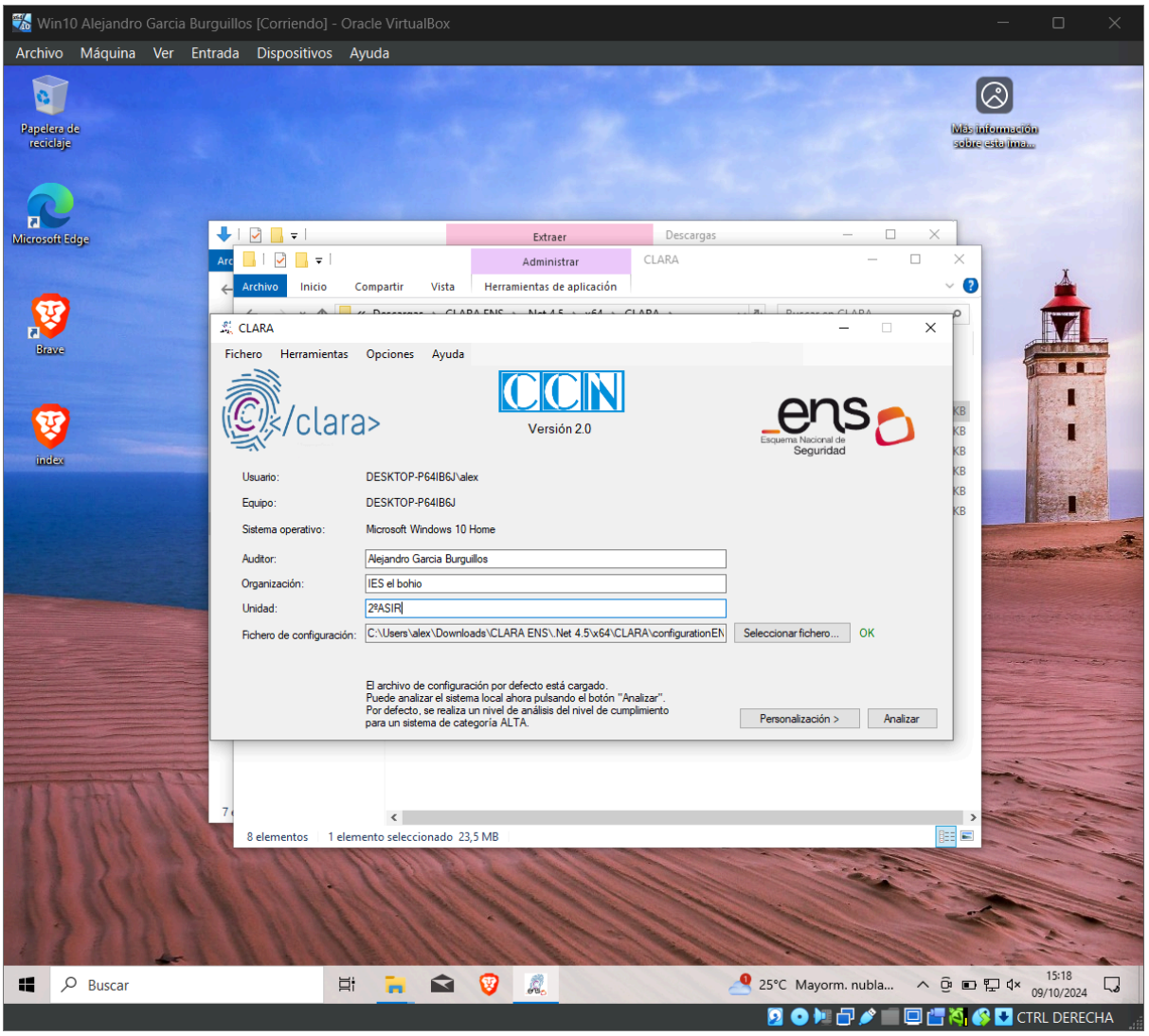
==========

[TIP]: Enhance Lynis audits by adding your settings to custom.prf (see /etc/lynis/default.prf for all settings)

PUNTO 2.

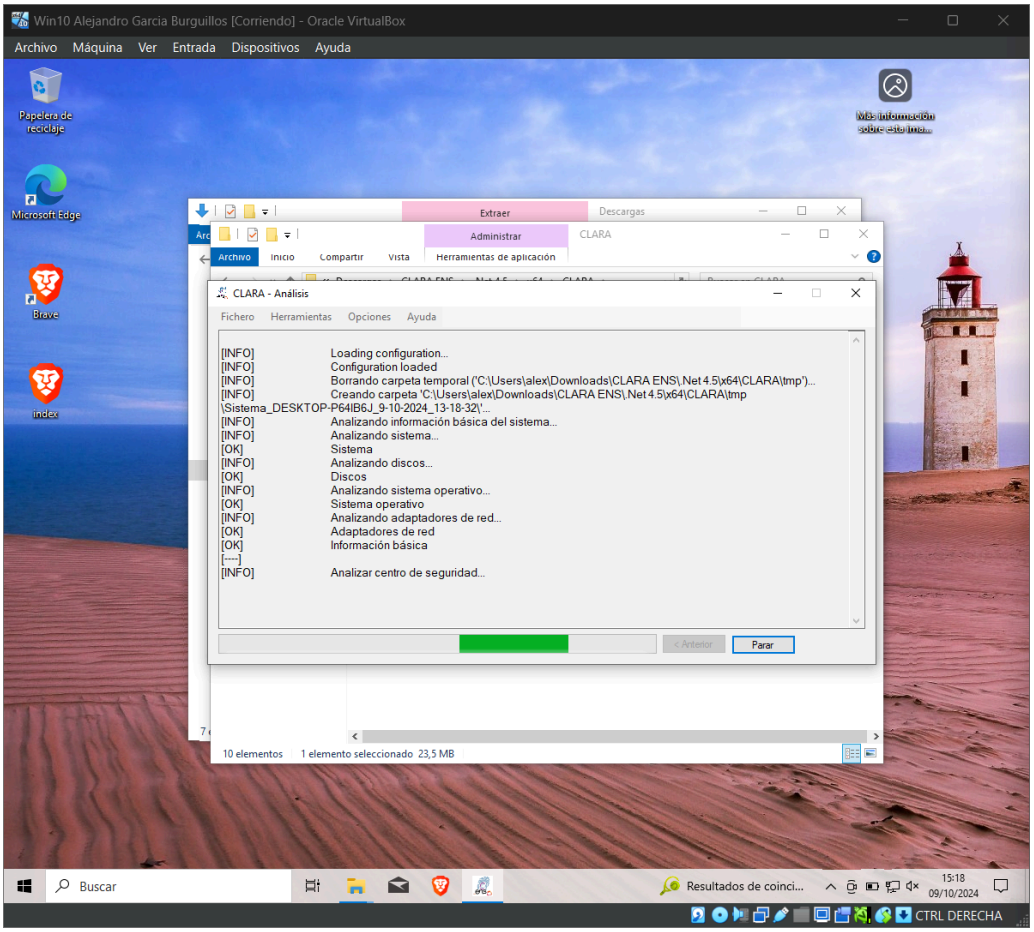
Ahora vamos a descargar CLARA, para ello vamos a windows, y en el buscador copiamos el siguiente enlace https://www.ccn-cert.cni.es/soluciones-seguridad/clara.html.

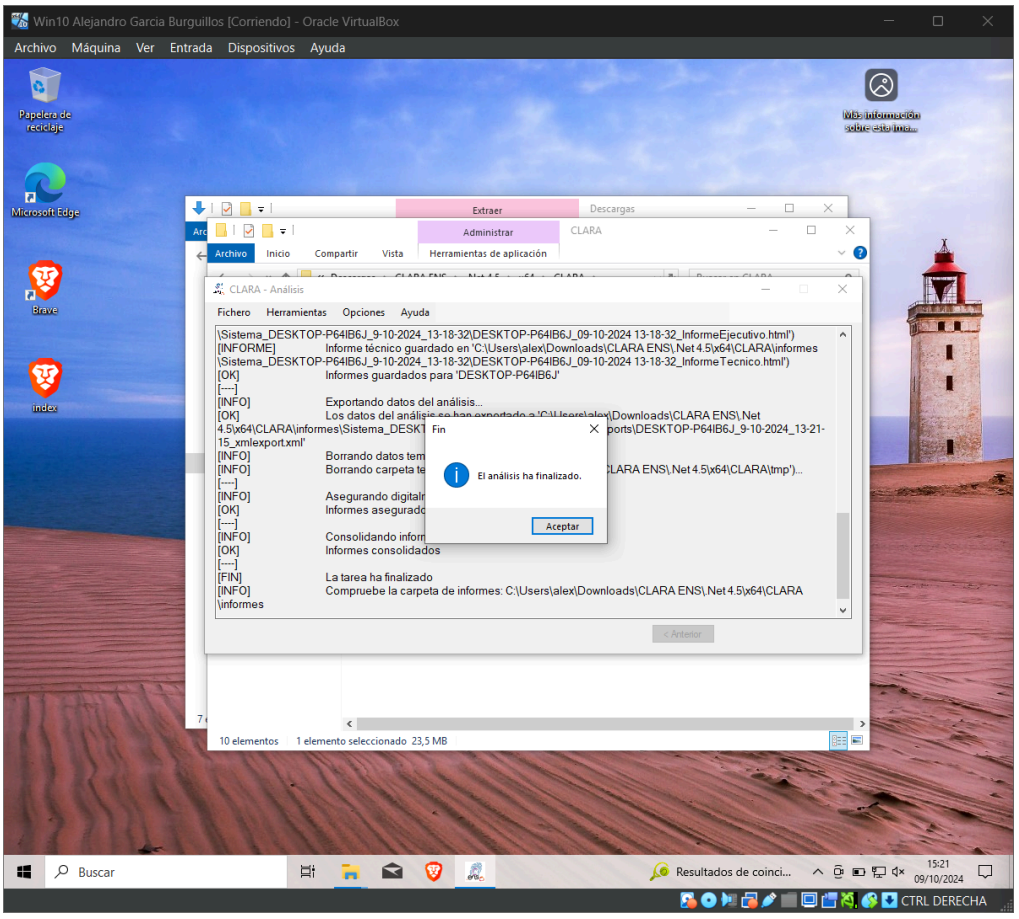
Una vez descargado abrimos el ejecutable e instalamos, cuando terminemos la instalación se nos abrirá esta ventana:



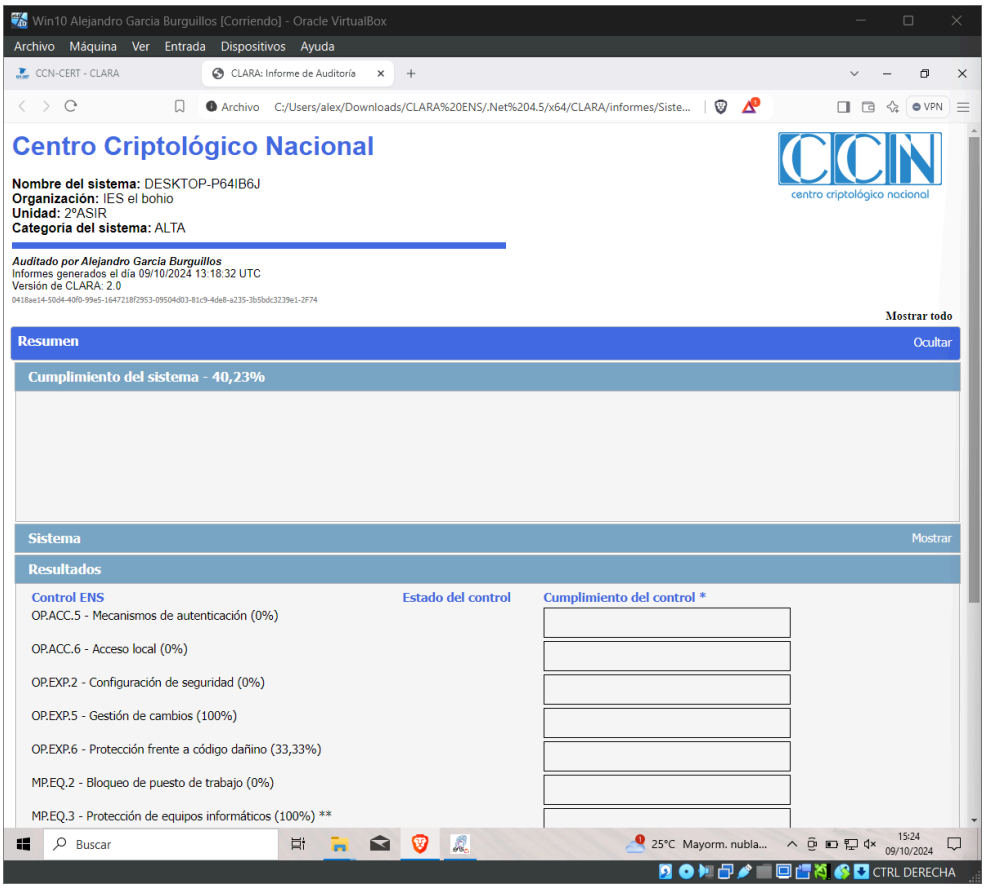
Aquí rellenamos con los datos deseados, en mi caso voy a poner lo mismo que mis compañeros, y le damos a Analizar.

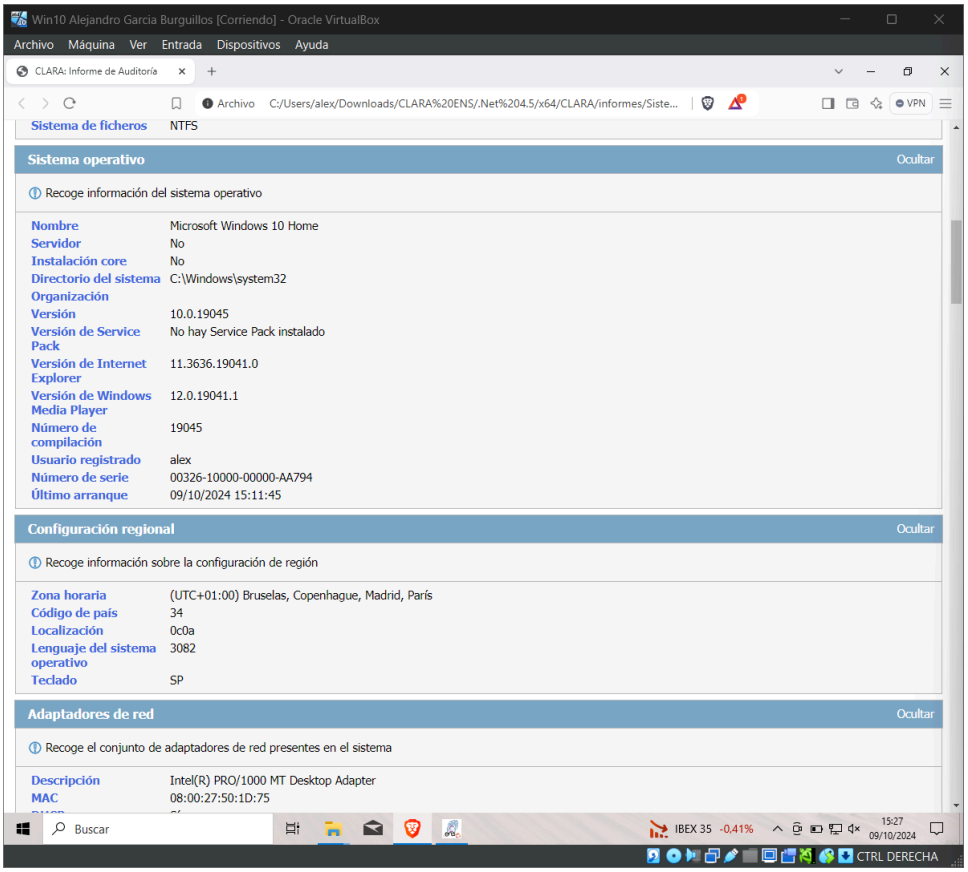
Empezará a realizar la auditoría del sistema lo que se vera asi:


Win10 Alejandro Garcia Burguillos [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Papelera de reciclaje
Microsoft Edge
Brave
index
Más información sobre esta ima...
CLARA - Análisis
Fichero Herramientas Opciones Ayuda
[INFO] Loading configuration...
[INFO] Configuration loaded
[INFO] Borrando carpeta temporal ('C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\tmp')...
[INFO] Creando carpeta 'C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\tmp\Sistema_DESKTOP-P64IB6J_9-10-2024_13-18-32\'...
[INFO] Analizando información básica del sistema...
[INFO] Analizando sistema...
[OK] Sistema
[INFO] Analizando discos...
[OK] Discos
[INFO] Analizando sistema operativo...
[OK] Sistema operativo
[INFO] Analizando adaptadores de red...
[OK] Adaptadores de red
[OK] Información básica
[----]
[INFO] Analizar centro de seguridad...
Anterior
Parar
10 elementos 1 elemento seleccionado 23,5 MB
Buscar
Resultados de coinci...
15:18
09/10/2024
CTRL DERECHA


Win10 Alejandro Garcia Burguillos [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Papelera de reciclaje
Microsoft Edge
Brave
index
Más información sobre esta ima...
CLARA - Análisis
Fichero Herramientas Opciones Ayuda
\Sistema_DESKTOP-P64IB6J_9-10-2024_13-18-32\DESKTOP-P64IB6J_09-10-2024 13-18-32_InformeEjecutivo.html')
[INFORME] Informe técnico guardado en 'C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\informes\Sistema_DESKTOP-P64IB6J_9-10-2024_13-18-32\DESKTOP-P64IB6J_09-10-2024 13-18-32_InformeTecnico.html')
[OK] Informes guardados para 'DESKTOP-P64IB6J'
[----]
[INFO] Exportando datos del análisis...
[OK] Los datos del análisis se han exportado a 'C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\informes\Sistema_DESKTOP-P64IB6J_9-10-2024_13-21-15_xmlexport.xml'
[INFO] Borrando datos tem
[INFO] Borrando carpeta te
[----]
[INFO] Asegurando digitalr
[OK] Informes asegurado
[----]
[INFO] Consolidando inform
[OK] Informes consolidados
[----]
[FIN] La tarea ha finalizado
[INFO] Compruebe la carpeta de informes: C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\informes
Fin
El análisis ha finalizado.
Aceptar
Anterior
10 elementos 1 elemento seleccionado 23,5 MB
Buscar
Resultados de coinci...
15:21
09/10/2024
CTRL DERECHA

Aparta de la propia auditoría vista en la misma ventana nos dejara un archivo que podremos abrir con el navegador que también contendrá información de esta.





Auditoria Clara:

[INFO] Loading configuration...

[INFO] Configuration loaded

[INFO] Borrando carpeta temporal ('C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\tmp')...

[INFO] Creando carpeta 'C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\tmp\Sistema_DESKTOP-P64IB6J_9-10-2024_13-21-49\'...

[INFO] Analizando información básica del sistema...

[INFO] Analizando sistema...

[OK] Sistema

[INFO] Analizando discos...

[OK] Discos

[INFO] Analizando sistema operativo...

[OK] Sistema operativo

[INFO] Analizando adaptadores de red...

[OK] Adaptadores de red

[OK] Información básica

[----]

[INFO] Analizar centro de seguridad...

[OK] Centro de seguridad

[----]

[INFO] Analizar plantilla de seguridad...

[INFO] Obteniendo información de la configuración local. Este proceso puede tardar varios minutos. Por favor, espere...

[OK] Información obtenida

[INFO] Comparando directivas...

[OK] Directivas comparadas

[INFO] Obteniendo y comparando información adicional de las directivas locales. Este proceso puede tardar varios minutos. Por favor, espere...

[OK] Información adicional obtenida

[INFO] Obteniendo y comprobando el cumplimiento del ENS en relación a las plantillas administrativas...

[OK] Plantillas administrativas del ENS obtenidas y comprobadas

[INFO] Creando carpeta 'C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\tmp\DESKTOP-P64IB6J\'...

[INFO] Comprobando cumplimiento de las directivas de seguridad del ENS...

[OK] Directivas de seguridad del ENS comprobadas

[----]

[INFO] Creando carpeta 'C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\informes\Sistema_DESKTOP-P64IB6J_9-10-2024_13-21-49'...

[INFORME] Informe ejecutivo guardado en 'C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\informes\Sistema_DESKTOP-P64IB6J_9-10-2024_13-21-49\DESKTOP-P64IB6J_09-10-2024 13-21-49_InformeEjecutivo.html')

[INFORME] Informe técnico guardado en 'C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\informes\Sistema_DESKTOP-P64IB6J_9-10-2024_13-21-49\DESKTOP-P64IB6J_09-10-2024 13-21-49_InformeTecnico.html')

[OK] Informes guardados para 'DESKTOP-P64IB6J'

[----]

[INFO] Exportando datos del análisis…

[OK] Los datos del análisis se han exportado a 'C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\informes\Sistema_DESKTOP-P64IB6J_9-10-2024_13-21-49\Exports\DESKTOP-P64IB6J_9-10-2024_13-24-9_xmlexport.xml'

[INFO] Borrando datos temporales...

[INFO] Borrando carpeta temporal ('C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\tmp')...

[----]

[INFO] Asegurando digitalmente los informes...

[OK] Informes asegurados digitalmente

[----]

[INFO] Consolidando informes...

[OK] Informes consolidados

[----]

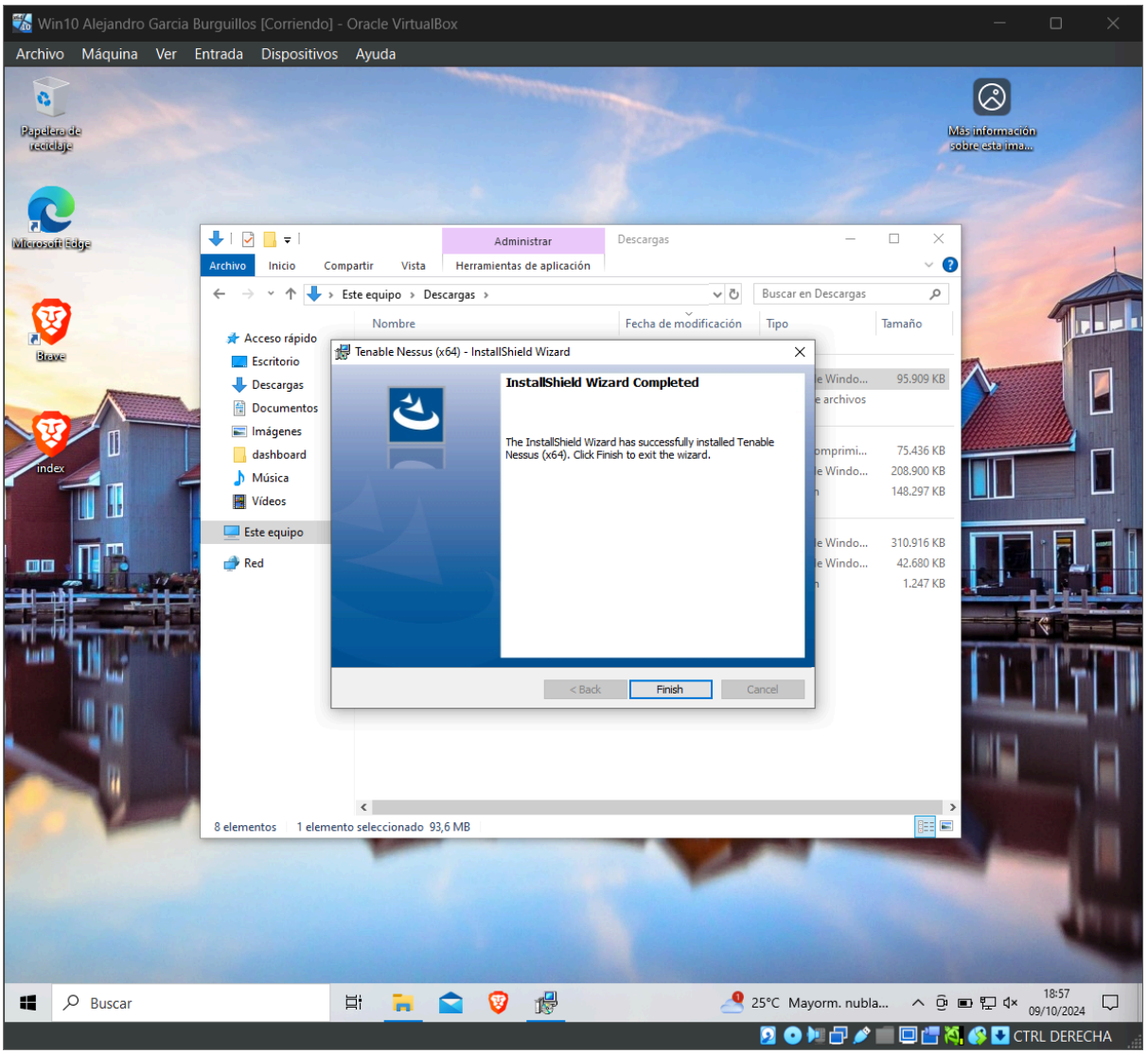
[FIN] La tarea ha finalizado

[INFO] Compruebe la carpeta de informes: C:\Users\alex\Downloads\CLARA ENS\.Net 4.5\x64\CLARA\informes

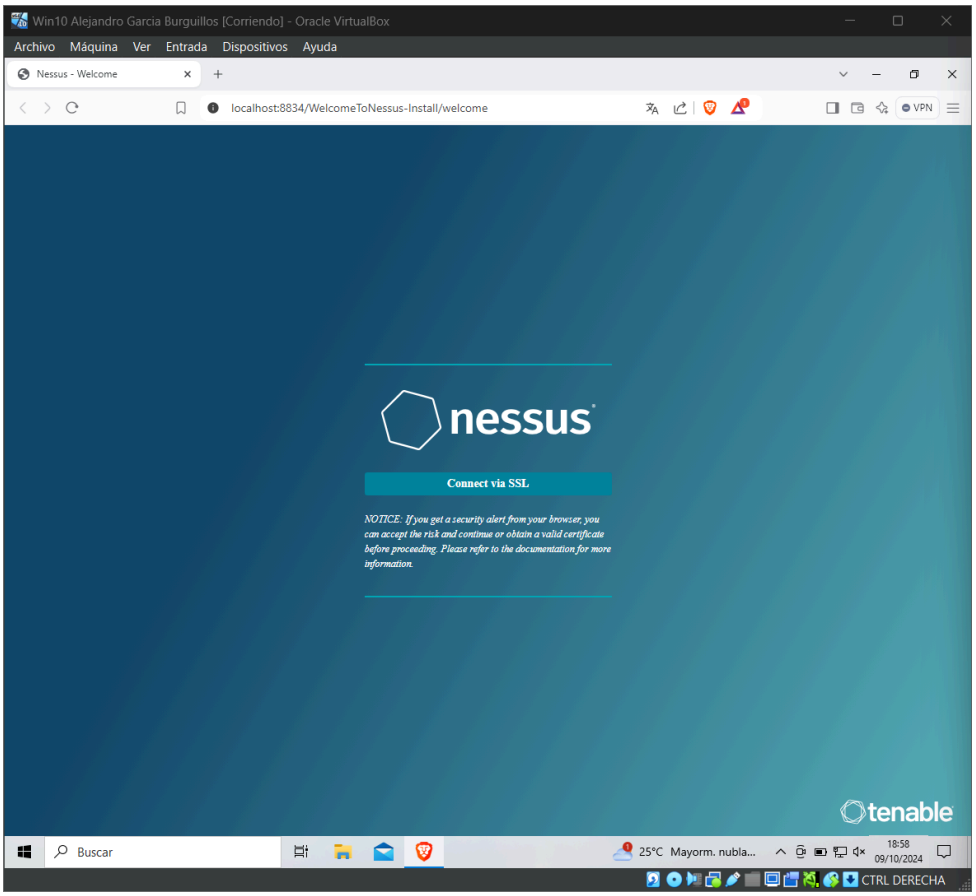
PUNTO 3.

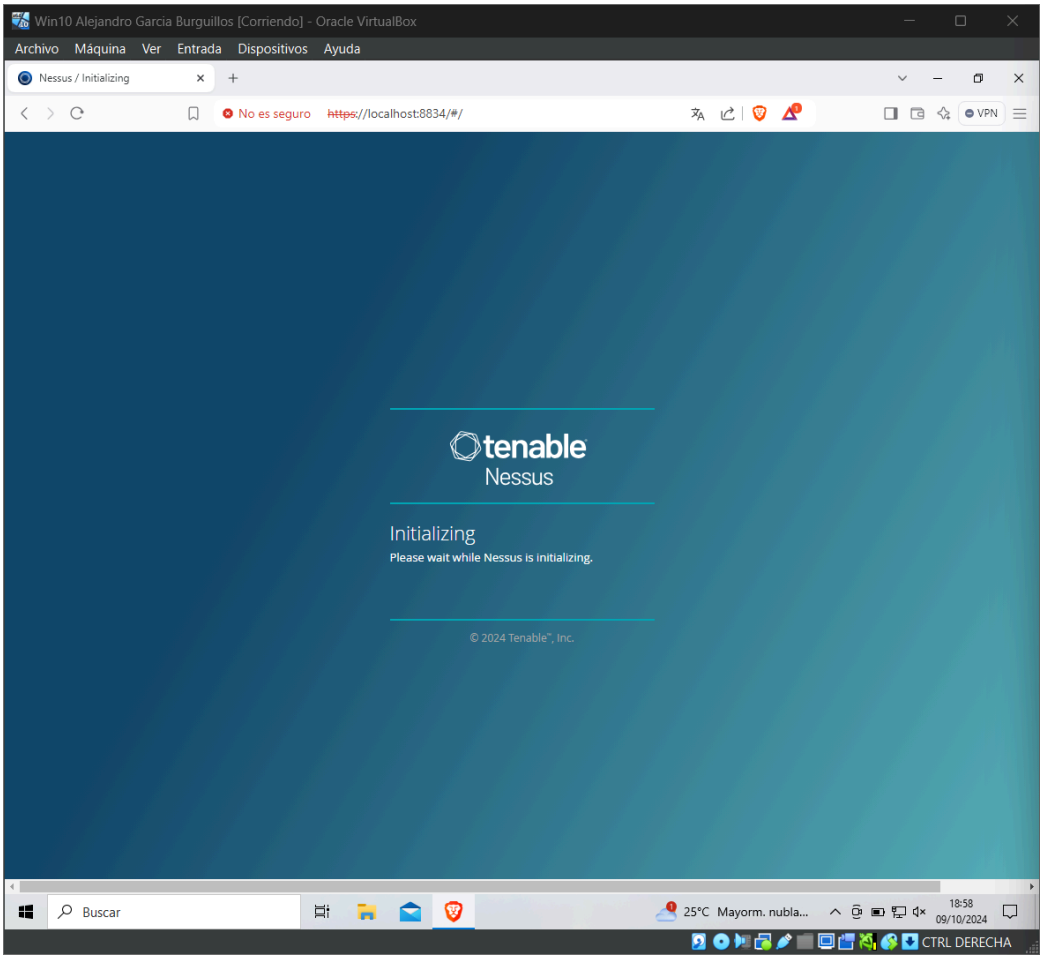
Por últimos la instalación de **Nessus,** en mi caso la voy a realizar en windows, para ello vamos al siguiente enlace
https://www.tenable.com/tenable-for-education/nessus-essentials

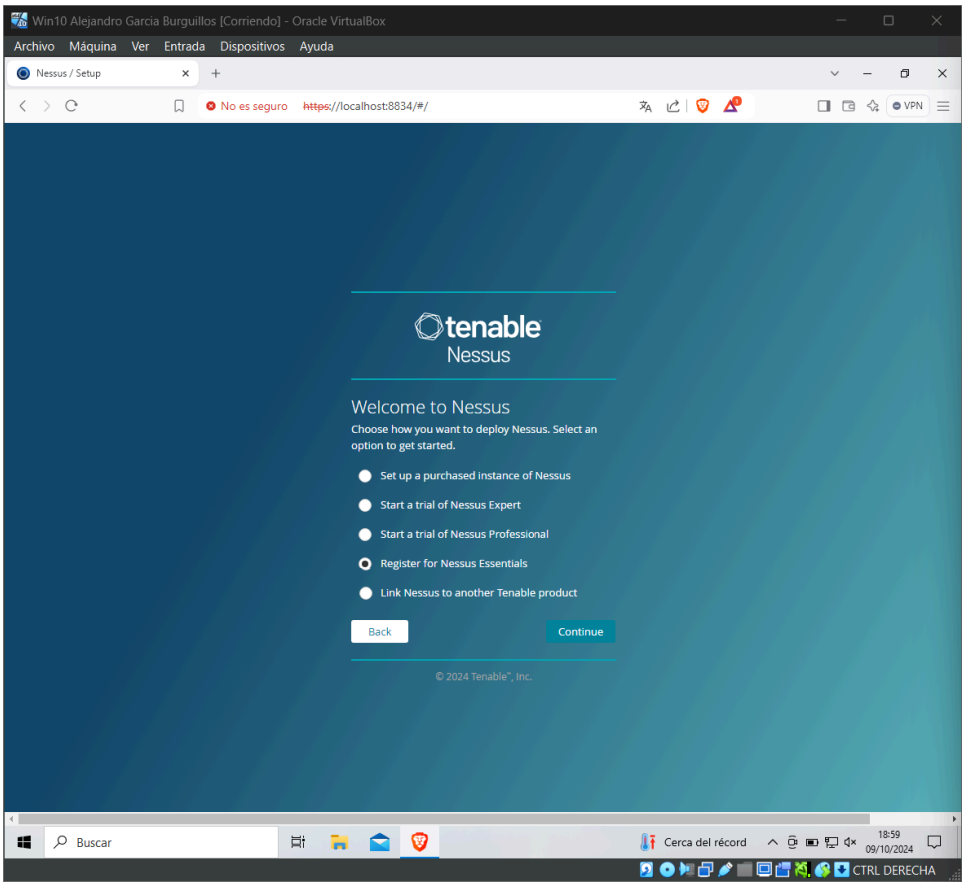
Para la instalación simplemente abrimos el ejecutable y le damos siguiente a todo hasta finalizar.

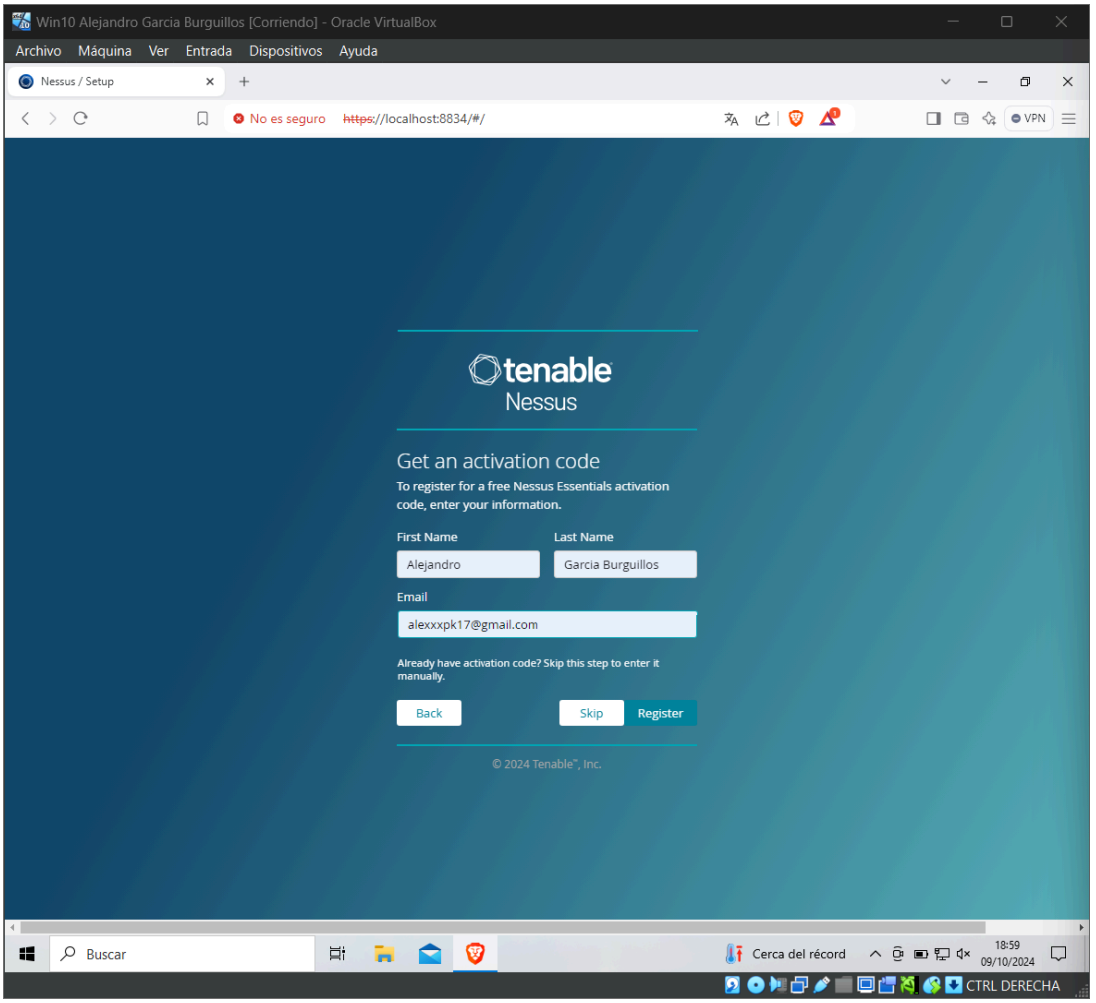


Cuando lleguemos al final simplemente le damos a Finish y se nos abrirá una ventana en el navegador.

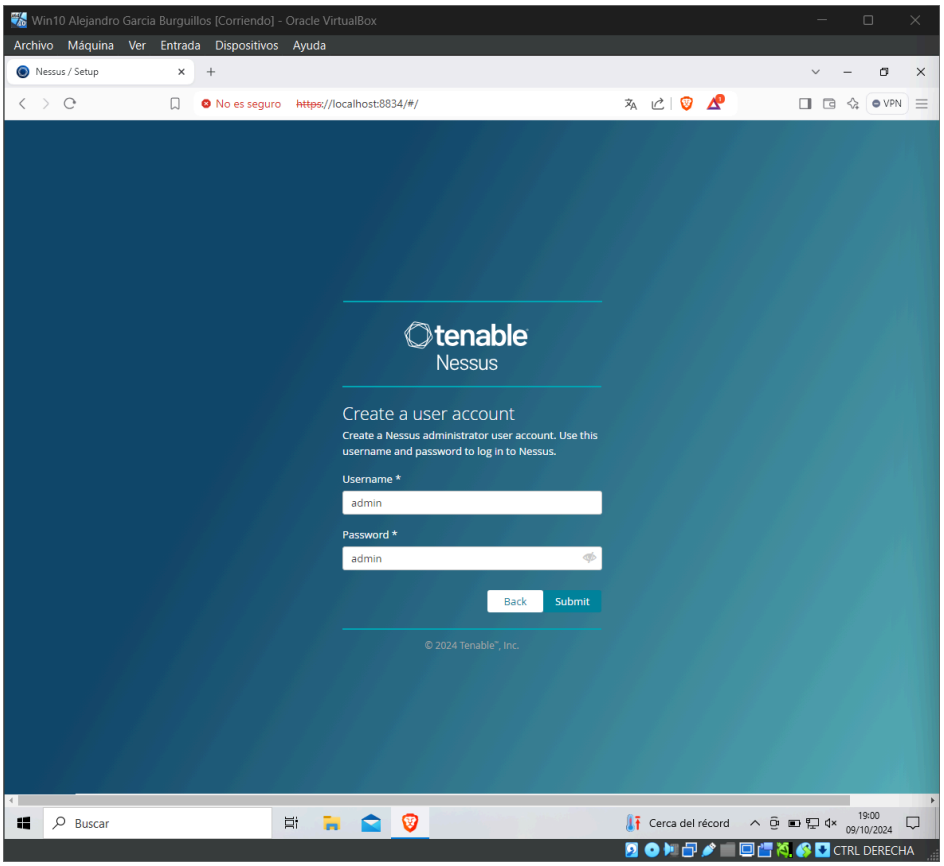

Win10 Alejandro Garcia Burguillos [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Nessus - Welcome
localhost:8834/WelcomeToNessus-Install/welcome
nessus
Connect via SSL
NOTICE: If you get a security alert from your browser, you can accept the risk and continue or obtain a valid certificate before proceeding. Please refer to the documentation for more information.
tenable
Buscar
25°C Mayorm. nubla...
18:58
09/10/2024
CTRL DERECHA

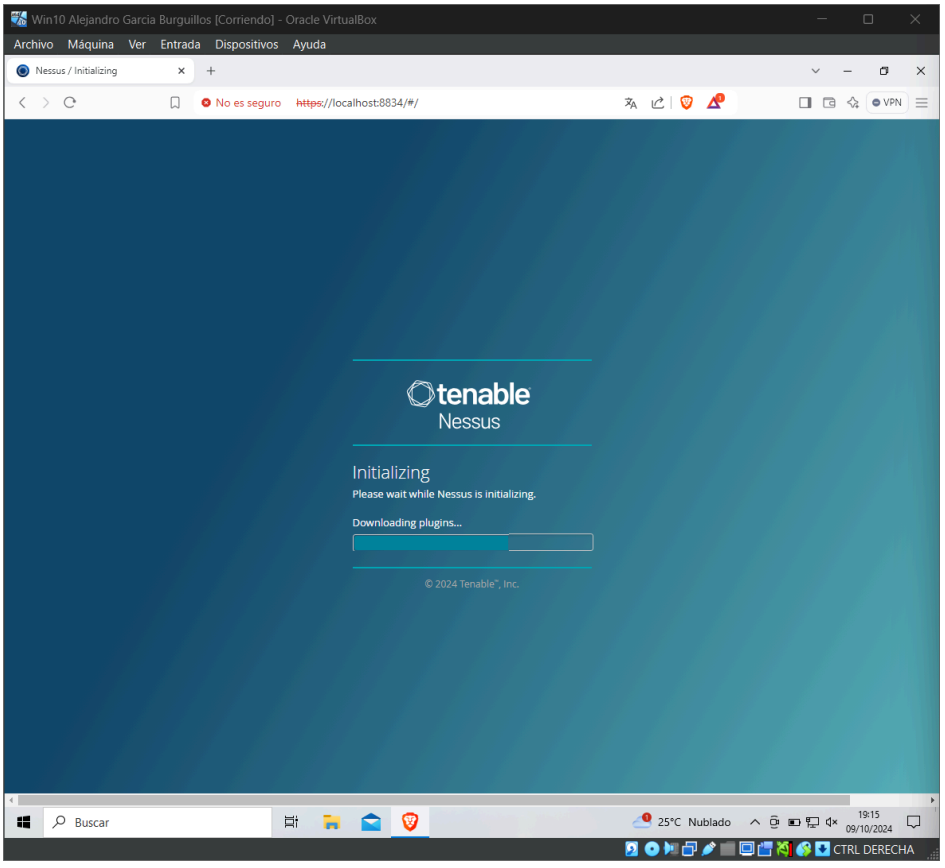

Win10 Alejandro Garcia Burguillos [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Nessus / Initializing
No es seguro https://localhost:8834/#/
tenable
Nessus
Initializing
Please wait while Nessus is initializing.
© 2024 Tenable™, Inc.
Buscar
25°C Mayorm. nubla...
18:58
09/10/2024
CTRL DERECHA


Win10 Alejandro Garcia Burguillos [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Nessus / Setup
No es seguro https://localhost:8834/#/
VPN
tenable
Nessus
Welcome to Nessus
Choose how you want to deploy Nessus. Select an option to get started.
Set up a purchased instance of Nessus
Start a trial of Nessus Expert
Start a trial of Nessus Professional
Register for Nessus Essentials
Link Nessus to another Tenable product
Back
Continue
© 2024 Tenable™, Inc.
Buscar
Cerca del récord
18:59
09/10/2024
CTRL DERECHA

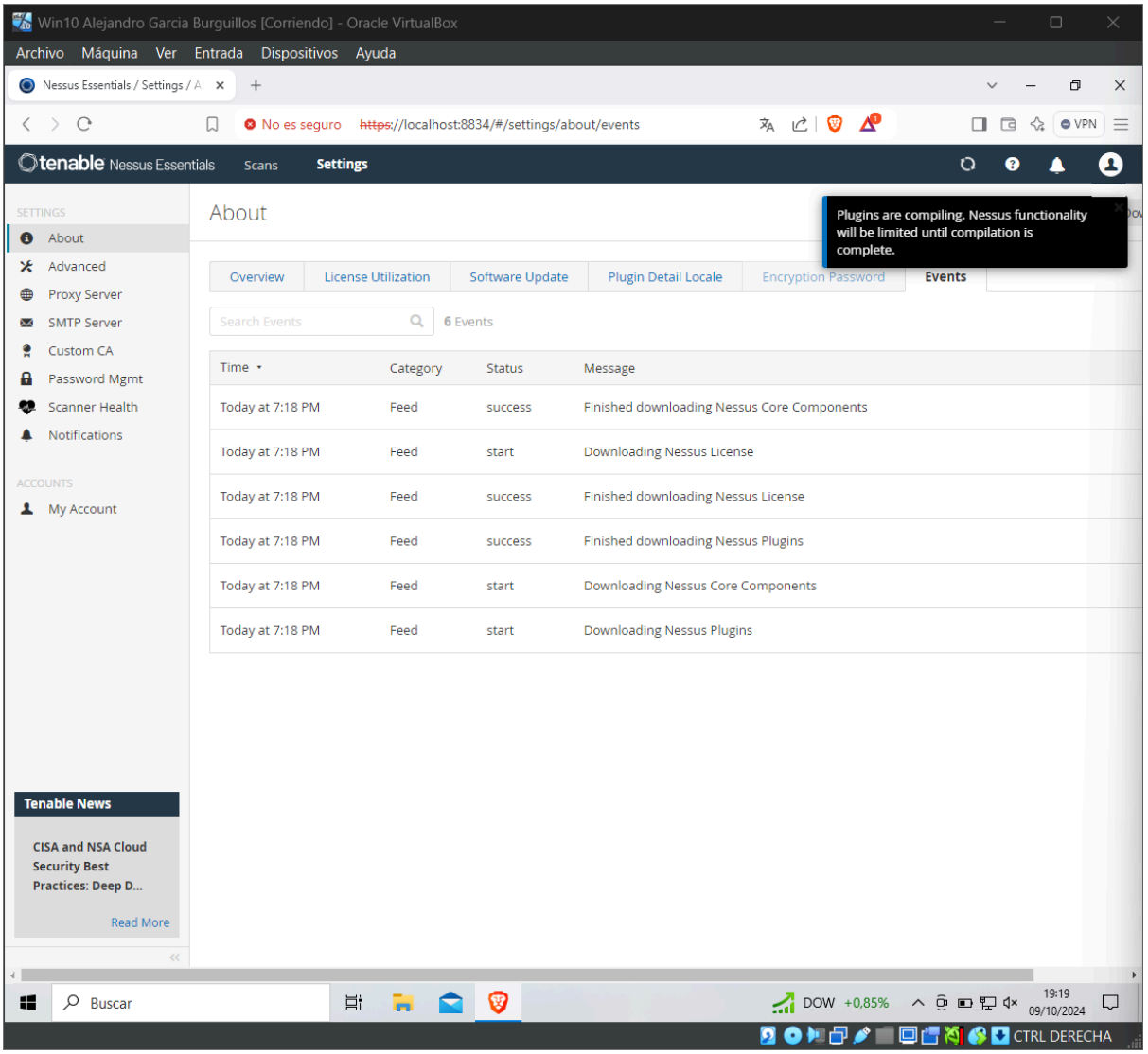

Win10 Alejandro Garcia Burguillos [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Nessus / Setup
No es seguro https://localhost:8834/#/
VPN
tenable
Nessus
Get an activation code
To register for a free Nessus Essentials activation code, enter your information.
First Name
Last Name
Alejandro
Garcia Burguillos
Email
alexxxpk17@gmail.com
Already have activation code? Skip this step to enter it manually.
Back
Skip
Register
© 2024 Tenable™, Inc.
Buscar
Cerca del récord
18:59
09/10/2024
CTRL DERECHA

Elegimos la tercera opción y rellenamos con los datos deseados, después de esto nos darán un código de activación de licencia que no necesitaremos usar para la realización de la tarea y nos pidieron crear un usuario, en mi caso admin admin.



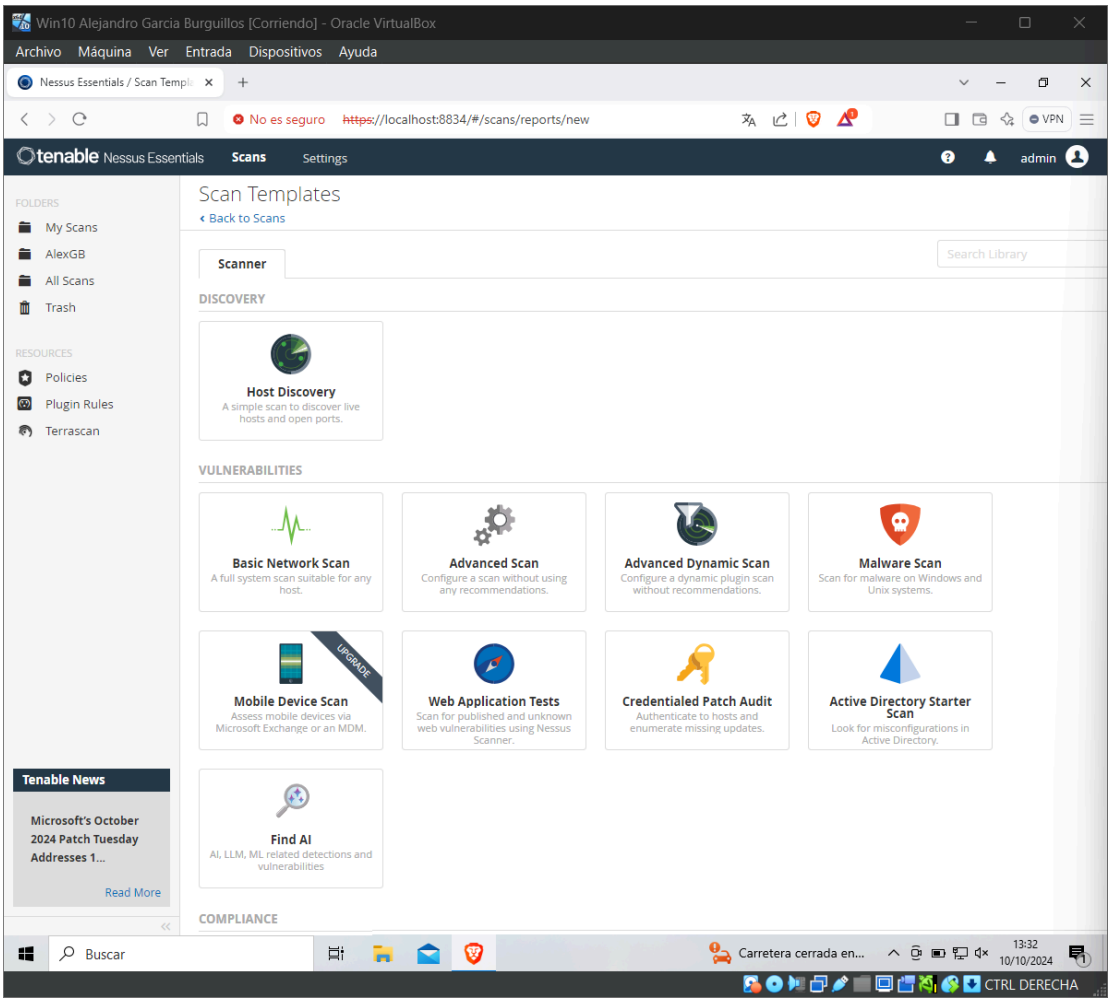


Cuando terminemos se pondrá a instalar otra vez, y cuando termine se pondrá a instalar otra vez más.

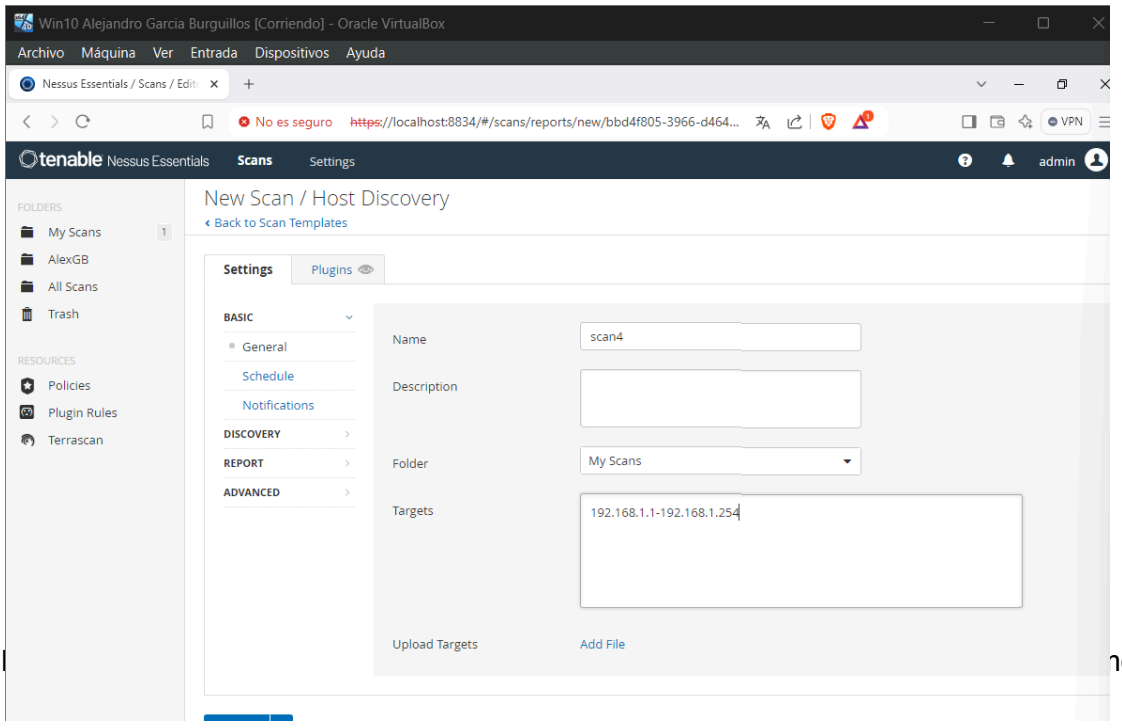


Una vez se quite la ruleta de la descarga ya lo tendremos todo instalado, ahora iremos a Scans y realizaremos uno.

Le damos a la primera opción que es la que usaremos para la tarea.



Una vez dentro encontraremos la siguiente pantalla, donde tendremos que poner el nombre que le queremos dar al escáner y el rango de ips en el que queremos que busque.



l nos

información útil como las vulnerabilidades de nuestra red y los dispositivos que están conectados a ella.

En mi caso por algún motivo solo me muestra el host, pero deberían salir todos los dispositivos conectados.